planning, coordination, and control of NASA programs is vested in NASA Headquarters located in Washington, DC. For additional information, visit *http://www.nasa.gov/about/org_index.html*.

[79 FR 18444, Apr. 2, 2014]

Subpart 3—Boards and Committees

§ 1201.300 Boards and committees.

(a) NASA's Contract Adjustment Board (CAB) and Inventions and Contributions Board (ICB) were established as part of the permanent organization structure of NASA. Charters for both Boards are set forth in part 1209 of this chapter. Procedures for the CAB are set out in 48 CFR part 1850, and procedures for the ICB are set out in 14 CFR parts 1240 and 1245.

(b) The Armed Services Board of Contract Appeals (ASBCA) is a neutral, independent forum whose primary function is to hear and decide post-award contract disputes between government contractors and those entities with whom the ASBCA has entered into agreement to provide services (NASA is one of those entities). The ASBCA functions in accordance with the Contract Disputes Act (41 U.S.C. 7101–7109), its Charter, or other remedy-granting provisions. Information about the ASBCA can be obtained by mail at ASBCA, Skyline 6, Suite 700, 5109 Leesburg Pike, Falls Church, Virginia 22041–3208, by phone at 703–681–8500, or from the Web at *www.asbca.mil*.

[79 FR 18444, Apr. 2, 2014]

Subpart 4 [Reserved]

PART 1203—INFORMATION SECURITY PROGRAM

Subpart A—Scope

Sec.
1203.100 Legal basis.
1203.101 Other applicable NASA regulations.

Subpart B—NASA Information Security Program

1203.200 Background and discussion.
1203.201 Information security objectives.
1203.202 Responsibilities.
1203.203 Degree of protection.

Subpart C—Classification Principles and Considerations

1203.300 General.
1203.301 Identification of information requiring protection.
1203.302 Compilation.
1203.303 Distribution controls.
1203.304 Internal effect.
1203.305 Restricted data.

Subpart D—Guides for Original Classification

1203.400 Specific classifying guidance.
1203.401 Effect of open publication.
1203.402 Classifying material other than documentation.
1203.403 [Reserved]
1203.404 Handling of unprocessed data.
1203.405 Proprietary information.
1203.406 Additional classification factors.
1203.407 Duration of classification.
1203.408 Assistance by Information Security Specialist in the Center Protective Services Office.
1203.410 Limitations.
1203.411 Restrictions.
1203.412 Classification guides.

Subpart E—Derivative Classification

1203.500 Use of derivative classification.
1203.501 Applying derivative classification markings.

Subpart F—Declassification and Downgrading

1203.600 Policy.
1203.601 Responsibilities.
1203.602 Authorization.
1203.603 Systematic review for declassification.
1203.604 Mandatory review for declassification.

Subpart G [Reserved]

Subpart H—Delegation of Authority To Make Determinations in Original Classification Matters

1203.800 Establishment.
1203.801 Responsibilites
1203.802 Membership.
1203.803 Ad hoc committees.
1203.804 Meetings.

Subpart I—NASA Information Security Program Committee

1203.900 Establishment.
1203.901 Responsibilities.
1203.902 Membership.
1203.903 Ad hoc committees.

Subpart J—Special Access Programs (SAP) and Sensitive Compartmented Information (SCI) Programs

AUTHORITY: E.O. 13526, E.O. 12968, E.O. 13549, E.O. 12829, 32 CFR part 2001, and 51 U.S.C., 20132, 20133.

SOURCE: 44 FR 34913, June 18, 1979, unless otherwise noted.

Subpart A—Scope

§ 1203.100 Legal basis.

(a) *Executive Order 13526 (hereinafter referred to as ''the Order'').* The responsibilities and authority of the Administrator of NASA with respect to the original classification of official information or material requiring protection against unauthorized disclosure in the interest of national defense or foreign relations of the United States (hereinafter collectively termed ''national security''), and the standards for such classification, are established by the ''the Order'' and the Information Security Oversight Office Directive No. 1, as amended (32 CFR part 2001, ''Classified National Security Information'');

(b) *E.O. 10865.* Executive Order 10865 (24 FR 1583) requires the Administrator to prescribe by regulation such specific requirements, restrictions and other safeguards as the Administrator may consider necessary to protect:

(1) Releases of classified information to or within United States industry that relate to contracts with NASA; and

(2) Other releases of classified information to industry that NASA has responsibility for safeguarding.

(c) *The National Aeronautics and Space Act.* (1) The National Aeronautics and Space Act (51 U.S.C. 20113) (Hereafter referred to as, ''The Space Act''), states:

> The Administrator shall establish such security requirements, restrictions, and safeguards as he deems necessary in the interest of the national security * * *

(2) Section 303 of the Space Act states:

> Information obtained or developed by the Administrator in the performance of his functions under this Act shall be made available for public inspection, except (i) information authorized or required by Federal statute to be withheld, and (ii) information classified to protect the national security: *Provided*, That nothing in this Act shall authorize the withholding of information by the Administrator from the duly authorized committees of the Congress.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5889, Feb. 9, 1983; 64 FR 72535, Dec. 28, 1999; 78 FR 5117, Jan. 24, 2013]

§ 1203.101 Other applicable NASA regulations.

(a) Subpart H of this part, ''Delegation of Authority to Make Determinations in Original Security Classification Matters.''

(b) Subpart I of this part, ''NASA Information Security Program Committee.''

(c) NASA Procedural Requirements (NPR) 1600.2, NASA Classified National Security Information (CNSI).

[44 FR 34913, June 18, 1979, as amended at 78 FR 5117, Jan. 24, 2013]

Subpart B—NASA Information Security Program

§ 1203.200 Background and discussion.

(a) In establishing a civilian space program, the Congress required NASA to ''provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof,'' and for the withholding from public inspection of that information that is classified to protect the national security.

(b) The Order was promulgated in recognition of the essential requirement for an informed public concerning the activities of its Government, as well as the need to protect certain national security information from unauthorized disclosure. It delegates to NASA certain responsibility for matters pertaining to national security and confers on the Administrator of NASA, or such responsible officers or employees as the Administrator may designate, the authority for original classification of official information or material which requires protection in the interest of national security. It also provides for:

(1) Basic classification, downgrading and declassification guidelines;

(2) The issuance of directives prescribing the procedures to be followed in safeguarding classified information or material;

(3) A monitoring system to ensure the effectiveness of the Order;

(4) Appropriate administrative sanctions against officers and employees of the United States Government who are found to be in violation of the Order or implementing directive; and

(5) Classification limitations and restrictions as discussed in §§ 1203.410 and 1203.411.

(c) The Order requires the timely identification and protection of that NASA information the disclosure of which would be contrary to the best interest of national security. Accordingly, the determination in each case must be based on a judgment as to whether disclosure of information could reasonably be expected to result in damage to the national security.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5889, Feb. 9, 1983; 78 FR 5117, Jan. 24, 2013]

§ 1203.201 Information security objectives.

The objectives of the NASA Information Security Program are to:

(a) Ensure that information is classified only when a sound basis exists for such classification and only for such period as is necessary.

(b) Prevent both the unwarranted classification and the overclassification of NASA information.

(c) Ensure the greatest practicable uniformity within NASA in the classification of information.

(d) Ensure effective coordination and reasonable uniformity with other Government departments and agencies, particularly in areas where there is an exchange or sharing of information, techniques, hardware, software, or other technologies.

(e) Provide a timely and effective means for downgrading or declassifying information when the circumstances necessitating the original classification change or no longer exist.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5117, Jan. 24, 2013]

§ 1203.202 Responsibilities.

(a) The Chairperson, NASA Information Security Program Committee (NISPC) (Subpart I of this part), who is the Assistant Administrator for Protective Services, or designee, is responsible for:

(1) Directing the NASA Information Security Program (NISP) in accordance with NASA policies and objectives and applicable laws and regulations.

(2) Ensuring effective compliance with and implementation of ''the Order'' and the Information Security Oversight Office Directive No. 1 relating to security classification matters.

(3) Reviewing, in consultation with the NASA Information Security Program Committee NISPC, questions, suggestions, appeals and compliance concerning the NISP and making determinations concerning them.

(4) Coordinating NASA security classification matters with NASA Centers and component facilities and other Government agencies.

(5) Ensuring Security Classification Guides for NASA are developed for NASA programs and projects.

(6) Developing, maintaining and recommending to the Administrator guidelines for the systematic review covering all classified information under NASA's jurisdiction.

(7) Reviewing and coordinating with appropriate offices all appeals of denials of requests for records under sections 552 and 552a of Title 5, United States Code (Freedom of Information and Privacy Acts) when the denials are based on the records' continued classification.

(8) Recommending to the Administrator appropriate administrative action to correct abuse or violations of any provision of the NISP, including notifications by warning letter, formal reprimand and to the extent permitted by law, suspension without pay and removal.

(b) All NASA employees are responsible for bringing to the attention of the Chairperson of the NISPC any information security problems in need of resolution, any areas of interest wherein information security guidance is lacking, and any other matters likely to impede achievement of the objectives prescribed in this section.

(c) Each NASA official to whom the authority for original classification is delegated shall be accountable for the propriety of each classification (see subpart H) and is responsible for:

(1) Ensuring that classification determinations are consistent with the policy and objectives prescribed above, and other applicable guidelines.

(2) Bringing to the attention of the Chairperson, NISPC, for resolution, any disagreement with classification determinations made by other NASA officials.

(3) Ensuring that information and material which no longer requires its present level of protection is promptly downgraded or declassified in accordance with applicable guidelines within a reasonable period.

(d) Other supervisors of NASA offices are responsible for:

(1) Ensuring that classified information or material prepared within their respective offices is appropriately marked.

(2) Ensuring that material proposed for public release is reviewed to redact classified information contained therein.

(e) Chiefs of Protective Services at NASA Centers are responsible for:

(1) Developing proposed Security Classification Guides and submitting the guide to the Office of Protective Services for review and approval.

(2) Ensuring that classified information or material prepared in their respective Center is appropriately marked.

(3) Ensuring that material proposed for public release is reviewed to redact classified information.

(4) Coordinating all security classification actions with the Center's Protective Services Office.

(f) The Director of the Office of Protective Services, NASA Headquarters, who serves as a member and Executive Secretary of the NISPC, is responsible for the NASA-wide coordination of security classification matters.

(g) The Information Security Program Manager, Office of Protective Services (OPS), is responsible for establishing procedures for the safeguarding of classified information or material (e.g., accountability, control, access, storage, transmission, and marking) and for ensuring that such procedures are systematically reviewed; and those which are duplicative or unnecessary are eliminated.

[44 FR 34913, June 18, 1979, as amended at 45 FR 3888, Jan. 21, 1980; 48 FR 5890, Feb. 9, 1983; 53 FR 41318, Oct. 21, 1988; 64 FR 72535, Dec. 28, 1999; 78 FR 5117, Jan. 24, 2013]

§ 1203.203 Degree of protection.

(a) *General.* Upon determination that information or material must be classified, the degree of protection commensurate with the sensitivity of the information must be determined. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within 30 days.

(b) *Authorized categories of classification.* The three categories of classification, as authorized and defined in ''the Order,'' are set out below. No other restrictive markings are authorized to be placed on NASA classified documents or materials except as expressly provided by statute or by NASA Directives.

(1) *Top Secret.* Top Secret is the designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

(2) *Secret.* Secret is the designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

(3) *Confidential.* Confidential is the designation applied to that information or material for which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5890, Feb. 9, 1983; 78 FR 5117, Jan. 24, 2013]

Subpart C—Classification Principles and Considerations

§ 1203.300 General.

In general, the types of NASA-generated information and material requiring protection in the interest of national security lie in the areas of applied research, technology or operations.

§ 1203.301 Identification of information requiring protection.

Classifiers shall identify the level of classification of each classified portion of a document (including subject and titles), and those portions that are not classified.

§ 1203.302 Compilation.

A compilation of items that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that meets the standards of classification under the Order; and is not otherwise revealed in the individual items of information. As used in the Order, compilations mean an aggregate of preexisting unclassified items of information.

[78 FR 5118, Jan. 24, 2013]

§ 1203.303 Distribution controls.

NASA shall establish controls over the distribution of classified information to ensure that it is dispersed only to organizations or individuals eligible for access to such information and with a need-to-know the information.

[78 FR 5118, Jan. 24, 2013]

§ 1203.304 Internal effect.

The effect of security protection on program progess and cost and on other functional activities of NASA should be considered. Impeditive effects and added costs inherent in a security classification must be assessed and weighed against the detrimental effects on the national security interests which would result from failure to classify.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.305 Restricted data.

Restricted Data or Formerly Restricted Data is so classified when originated or by operation of the law, as required by the Atomic Energy Act of 1954, as amended. Specific guidance for the classification of Restricted Data and Formerly Restricted Data is provided in ''Classification Guides'' published by the Department of Energy and or Department of Defense.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

Subpart D—Guides for Original Classification

§ 1203.400 Specific classifying guidance.

Technological and operational information and material, and in some exceptional cases scientific information falling within any one or more of the following categories, must be classified if its unauthorized disclosure could reasonably be expected to cause some degree of damage to the national security. In cases where it is believed that a contrary course of action would better serve the national interests, the matter should be referred to the Chairperson, NISPC, for a determination. It is not intended that this list be exclusive; original classifiers are responsible for initially classifying any other type of information which, in their judgment, requires protection under §1.4 of ''the Order.''

(a) Military plans, weapons systems, or operations;

(b) Foreign government information;

(c) Intelligence activities (including covert activities), intelligence sources or methods, or cryptology;

(d) Foreign relations or foreign activities of the United States, including confidential sources;

(e) Scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) The development, production, or plans relating to the use of weapons of mass destruction.

[78 FR 5118, Jan. 24, 2013]

§ 1203.401 Effect of open publication.

Public disclosure, regardless of source or form, of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosure requires an immediate reevaluation to determine whether the information has been compromised to the extent that downgrading or declassification is indicated. Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. In these cases, if a release were made or authorized by an official Government source, classification of clearly identified items may no longer be warranted. Questions as to the propriety of continued classification should be referred to the Chairperson, NASA Information Security Program Committee.

§ 1203.402 Classifying material other than documentation.

Items of equipment or other physical objects may be classified only where classified information may be derived by visual observation of internal or external appearance, structure, operation, test, application or use. The overall classification assigned to equipment or objects shall be at least as high as the highest classification of any of the items of information which may be revealed by the equipment or objects, but may be higher if the classifying authority determines that the sum of classified or unclassified information warrants such higher classification. In every instance where classification of an item of equipment or object is determined to be warranted, such determination must be based on a finding that there is at least one aspect of the item or object which requires protection. If mere knowledge of the existence of the equipment or object would compromise or nullify the reason or justification for its classification, the fact of its existence should be classified.

§ 1203.403 [Reserved]

§ 1203.404 Handling of unprocessed data.

It is the usual practice to withhold the release of raw scientific data received from spacecraft until it can be calibrated, correlated and properly interpreted by the experimenter under the monitorship of the cognizant NASA office. During this process, the data are withheld through administrative measures, and it is not necessary to resort to security classification to prevent premature release. However, if at any time during the processing of raw data it becomes apparent that the results require protection under the criteria set forth in this subpart D, it is the responsibility of the cognizant NASA office to obtain the appropriate security classification.

§ 1203.405 Proprietary information.

Proprietary information made available to NASA is subject to examination for classification purposes under the criteria set forth in this subpart D. Where the information is in the form of a proposal and accepted by NASA for support, it should be categorized in accordance with the criteria of § 1203.400. If NASA does not support the proposal but believes that security classification would be appropriate under the criteria of § 1203.400 if it were under Government jurisdiction, the contractor should be advised of the reasons why safeguarding would be appropriate, unless security considerations preclude release of the explanation to the contractor. NASA should identify the Government department, agency or activity whose national security interests might be involved and the contractor should be instructed to protect the proposal as though classified pending further advisory classification opinion by the Government activity whose interests are involved. If such a Government activity cannot be identified, the contractor should be advised that the proposal is not under NASA jurisdiction for classification purposes, and that the information should be sent, under proper safeguards, to the

Director, Information Security Oversight Office for a determination.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.406 Additional classification factors.

In determining the appropriate classification category, the following additional factors should be considered:

(a) *Uniformity within government activities.* The effect classification will have on technological programs of other Government departments and agencies should be considered. Classification of official information must be reasonably uniform within the Government.

(b) *Applicability of classification directives of other Government agencies.* It is necessary to determine whether authoritative classification guidance exists elsewhere for the information under consideration which would make it necessary to assign a higher classification than that indicated by the applicable NASA guidance. The Office of Protective Services will coordinate with the Information Security Oversight Office (ISOO) Committee and the National Declassification Center to determine what classification guides are current.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.407 Duration of classification.

(a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the timeframe established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this Order are followed.

(d) No information may remain classified indefinitely. Information that is marked for an indefinite duration of classification under predecessor orders, for example, information marked as ''Originating Agency's Determination Required,'' or classified information that contains either incomplete or no declassification instructions, shall have appropriate declassification information applied in accordance with part 3 of this order.

[78 FR 5118, Jan. 24, 2013]

§ 1203.408 Assistance by Information Security Specialist in the Center Protective Services Office.

Center Security Classification Officers, as the Center point-of-contact, will assist Center personnel in:

(a) Interpreting security classification guides and classification assignments for the Center.

(b) Answering questions and considering suggestions concerning security classification matters.

(c) Ensuring a continuing review of classified information for the purpose of declassifying or downgrading in accordance with subpart E of this part.

(d) Reviewing and approving, as the representative of the contracting officer, the DD Form 254, Contract Security Classification Specification, issued to contractors by the Center.

(e) Forwarding all security classification guides to the Office of Protective Services, NASA Headquarters, for final approval.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.409 Exceptional cases.

(a) In those cases where a person not authorized to classify information originates or develops information which is believed to require classification, that person must contact the Center's or installation's Information Security Officer in the Protective Services Office to arrange for proper review and safeguarding. Persons other than NASA employees should forward the information to the NASA Central Registry at 300 E Street SW., Washington, DC 20546, Attention: Office of Protective Services.

(b) Information in which NASA does not have primary interest shall be returned promptly, under appropriate safeguards, to the sender in accordance with § 1203.405.

(c) Material received from another agency for a NASA security classification determination shall be processed within 90 days. If a classification cannot be determined during that period, the material shall be sent, under appropriate safeguards, to the Director, Information Security Oversight Office, for a determination.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.410 Limitations.

(a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

(1) Conceal violations of law, inefficiency, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition; or

(4) Prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after declassification after being released to the public under proper authority unless: The reclassification is based on a document-by-document review by NASA and a determination that reclassification is required to prevent at least significant damage to the national security and personally approved in writing by the Administrator, the Deputy Administrator, or the Assistant Administrator for Protective Services. All reclassification actions will be coordinated with the Information Security Oversight Office before final approval; the information may be reasonably recovered without bringing undue public attention to the information; the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (the National Security Advisor) and the Director of the Information Security Oversight Office; and for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the Administrator, the Deputy Administrator, or the Assistant Administrator for Protective Services, after making the determinations required by this paragraph, shall notify the Archivist of the United States (hereafter, Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this Order only if such classification meets the requirements of this Order and is accomplished by document-by-document review with the personal participation or under the direction of the Administrator, the Deputy Administrator, or the Assistant Administrator for Protective Services. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance

with a specific date or event determined by an original classification authority in accordance with section 1.5 of this Order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) Meets the standards for classification under this Order; and

(2) Is not otherwise revealed in the individual items of information.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5890, Feb. 9, 1983; 78 FR 5119, Jan. 24, 2013]

§ 1203.411 Restrictions.

(a) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this section, the Department of Defense shall be considered one agency.

(b) Classified information shall not be disseminated outside the Executive Branch except under conditions that ensure the information will be given protection equivalent to that afforded within the Executive Branch.

[48 FR 5890, Feb. 9, 1983]

§ 1203.412 Classification guides.

(a) *General.* A classification guide, based upon classification determinations made by appropriate program and classification authorities, shall be issued for each classified system, program or project. Classification guides shall:

(1) Identify the information elements to be protected, using categorization and subcategorization to the extent necessary to ensure that the information involved can be readily and uniformly identified.

(2) State which of the classification designations (i.e., Top Secret, Secret or Confidential) apply to the identified information elements.

(3) State the duration of each specified classification in terms of a period of time or future event. If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires it be marked for declassification for up to 25 years from the date of the original decision.

(4) Indicate specifically that the designations, time limits, markings and other requirements of ''the Order'' are to be applied to information classified pursuant to the guide.

(5) All security classification guides should be forwarded to the Office of Protective Services for review and final approval. The Office of Protective Services will maintain a list of all classification guides in current use.

(b) *Review of classification guides.* Classification guides shall be reviewed by the originator for currency and accuracy not less than once every five years. Changes shall be in strict conformance with the provisions of this part 1203 and shall be issued promptly. If no changes are made, the originator shall so annotate the record copy and show the date of the review.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5891, Feb. 9, 1983; 78 FR 5119, Jan. 24, 2013]

Subpart E—Derivative Classification

§ 1203.500 Use of derivative classification.

(a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) Be identified by name and position or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) Observe and respect original classification decisions; and

(3) Carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple

sources, the derivative classifier shall carry forward:

(i) The date or event for declassification that corresponds to the longest period of classification among the sources or the marking established pursuant to section 1.6(a)(4)(D) of the Order; and

(ii) A listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum when classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the Order, with an emphasis on avoiding over-classification, at least once every two years. Derivative classifiers who do not receive such training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the Administrator, the Deputy Administrator, or the Assistant Administrator for Protective Services if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

[78 FR 5119, Jan. 24, 2013]

§ 1203.501 Applying derivative classification markings.

Persons who apply derivative classification markings shall:

(a) Observe and respect original classification decisions:

(b) Verify the information's current level of classification so far as practicable before applying the markings; and

(c) Carry forward to newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5891, Feb. 9, 1983]

Subpart F—Declassification and Downgrading

§ 1203.600 Policy.

Information shall be declassified or downgraded as soon as national security considerations permit. NASA reviews of classified information shall be coordinated with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by § 1203.400 despite the passage of time will continue to be protected in accordance with ''the Order.''

[48 FR 5891, Feb. 9, 1983]

§ 1203.601 Responsibilities.

Authorized officials with Declassification Authority (DCA) may declassify or downgrade information that is subject to the final classification jurisdiction of NASA and shall take such action in accordance with the provisions of this subpart F.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5120, Jan. 24, 2013]

§ 1203.602 Authorization.

Information shall be declassified or downgraded by an authorized DCA official. If that official is still serving in the same position, the originator's successor, a supervisory official of either, or officials delegated such authority in writing by the Administrator or the Chairperson, NISPC, may also make a decision to declassify or downgrade information.

[78 FR 5120, Jan. 24, 2013]

§ 1203.603 Systematic review for declassification:

(a) *General.* (1) NASA must establish and conduct a program for systematic declassification review of NASA-originated records of permanent historical value exempted from automatic declassification under section 3.3 of this Order. The NASA Office of Protective Services shall prioritize the review of

such records in coordination with the Center Protective Service Offices.

(2) The Archivist shall conduct a systematic declassification review program for classified records:

(i) Accessioned into the National Archives;

(ii) Transferred to the Archivist pursuant to 44 U.S.C. 2203; and

(iii) For which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

(3) The Chairperson, NISPC, shall designate experienced personnel to assist the Archivist in the systematic review of U.S. originated information and foreign information exempted from automated declassification. Such personnel shall:

(i) Provide guidance and assistance to the National Archives and Records Service in identifying and separating documents and specific categories of information within documents which are deemed to require continued classification; and

(ii) Develop reports of information or document categories so separated, with recommendations concerning continued classification.

(iii) Develop, in coordination with NASA organizational elements, guidelines for the systematic review for declassification of classified information under NASA's jurisdiction. The guidelines shall state specific limited categories of information which, because of their national security sensitivity, should not be declassified automatically, but should be reviewed to determine whether continued protection beyond 25 years is needed. These guidelines are authorized for use by the Archivist and the Director of the Information Security Oversight Office, with the approval of the Senior Agency Official, which is the Assistant Administrator, Office of Protective Services, for categories listed in section 3.3 of the Order. These guidelines shall be reviewed at least every five years and revised as necessary, unless an earlier review for revision is requested by the Archivist. Copies of the declassification guidelines promulgated by NASA will be provided to the Information Security Oversight Office, National Archives and Records Administration (NARA). All security classified records exempt from automatic declassification, whether held in storage areas under installation control or in Federal Records Centers, will be surveyed to identify those requiring scheduling for future disposition.

(A) Classified information or material over which NASA exercises exclusive or final original classification authority and which is to be declassified in accordance with the systematic review guidelines shall be so marked.

(B) Classified information or material over which NASA exercises exclusive or final original classification authority and which, in accordance with the systematic review guidelines is to be kept protected, shall be listed by category by the responsible custodian and referred to the Chairperson, NASA Information Security Program Committee. This listing shall:

(*1*) Identify the information or material involved.

(*2*) Recommend classification beyond 25 years to a specific event scheduled to happen or a specific period of time in accordance with the Order.

(*3*) The Administrator shall delegate to the Senior Agency Official the authority to determine which category shall be kept classified and the dates or event for declassification.

(*4*) Declassification by the Director of the Information Security Oversight Office (DISOO). If the Director determines that NASA information is classified in violation of the Order, the Director may require the information to be declassified. Any such decision by the Director may be appealed through the NASA ISPC to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(b) [Reserved]

[78 FR 5120, Jan. 24, 2013]

§ 1203.604 Mandatory review for declassification.

(a) *Information covered.* Except as provided in paragraph (b) of this section, all information classified under the Order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) The request for a review describes the document or material containing

the information with sufficient specificity to enable the agency to locate it in a reasonably timely manner;

(2) The document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) The information is not the subject of pending litigation.

(b) *Presidential papers.* Information originated by the President or Vice President; the President's White House Staff, or the Vice President's Staff; committees, commissions, or boards appointed by the President; or other entities within the Executive Office of the President that solely advise and assist the President are exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a decision on the appeal.

(c) *Submission of requests for review.* Requests for mandatory review of classified information shall be submitted in accordance with the following:

(1) Requests originating within NASA shall, in all cases, be submitted directly to the NASA Office of Protective Services.

(2) For the most expeditious action, requests from other Governmental agencies or from members of the public should be submitted directly to the NASA Office of Protective Services only. The requestor may submit the request to: National Aeronautics and Space Administration (NASA), Central Registry, 300 E Street SW., Washington DC 20546, Attention: Office of Protective Services/Information Security Program Manager. The phrase, ''Mandatory Declassification Review,'' must be stated in the request.

(d) *Requirement for processing.* (1) Requests which are submitted under the Freedom of Information Act cannot be processed under the MDR process.

(2) The request describes the document or material containing the information with sufficient specificity, such as accession numbers, box titles or numbers, date and title of document, in any combination, to enable NASA to locate it with a reasonable amount of effort, not to exceed 30 days. If more time is required, NASA will notify the requester. After review, the information or any portion thereof that no longer requires protection shall be declassified and released unless withholding is otherwise warranted under applicable law.

(e) *Processing of requests.* Requests that meet the requirements of paragraph (d)(2) of this section will be processed as follows:

(1) The NASA Office of Protective Services review upon receiving the initial request shall be completed within 365 days.

(2) Receipt of the request shall be acknowledged promptly. The NASA Office of Protective Services shall determine whether, under the declassification provisions of this part 1203, the requested information may be declassified and, if so, shall make such information available to the requestor, unless withholding is otherwise warranted under applicable law. If the information may not be released in whole or in part, the requestor shall be given a brief statement of the reasons for denial, a notice of the right to appeal the determination to the Chairperson, NASA Information Security Program Committee, National Aeronautics and Space Administration, Washington, DC 20546, and a notice that such an appeal must be filed within 60 days in order to be considered.

(3) All appeals of denials of requests for declassification shall be acted upon and determined finally within 120 working days after receipt, and the requester shall be advised that the appeal

determination is final. If the requester is dissatisfied with NASA's appeal decision, the requester may initiate an appeal to the Interagency Security Classification Appeals Panel (ISCAP), within the Information Security Oversight Office. If continued classification is required under the provisions of this part 1203, the requester shall be notified of the reasons thereof.

(4) The declassification and release of foreign government information that is subjected to mandatory review under this section shall be determined only in accordance with §1203.703.

(5) When the NASA Office of Protective Services receives any request for declassification of information in documents in its custody that was classified by another Government agency, it shall refer copies of the request and the requested documents to the originating agency for processing and may, after consultation with the originating agency, inform the requester of the referral.

(f) *Neutral response.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of ''the Order,'' NASA shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under ''the Order.''

(g) *Declassification of transferred documents or material*—(1) *Material officially transferred.* In the case of classified information or material transferred by or pursuant to statute or Executive Order to NASA in conjunction with a transfer of functions (not merely for storage purposes) for NASA's use and as part of its official files or property, as distinguished from transfers merely for purposes of storage, NASA shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

(2) *Material not officially transferred.* When NASA has in its possession classified information or material originated by an agency which has since ceased to exist and that information has not been officially transferred to another department or agency or when it is impossible for NASA to identify the originating agency and a review of the material indicates that it should be downgraded or declassified, NASA shall be deemed to be the originating agency for the purpose of declassifying or downgrading such material. NASA will consult with the Information Security Oversight Office to assist in final disposition of the information.

(3) *Transfer for storage or retirement.* (i) Insofar as practicable, classified documents shall be reviewed to determine whether or not they can be downgraded or declassified prior to being forwarded to records centers or to the National Archives for storage. Any downgrading or declassification determination shall be indicated on each document by appropriate markings.

(ii) Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded or declassified by the Archivist of the United States in accordance with ''the Order,'' the directives of the Information Security Oversight Office, GSA, and NASA guidelines.

(h) *Downgrading and declassification actions*—(1) *Notification of changes in classification or declassification.* When classified material has been marked with specific dates or events for downgrading or declassification, it is not necessary to issue notices of such actions to any holders. However, when such actions are taken earlier than originally scheduled, or the duration of classification is shortened, the authority making such changes shall, to the extent practicable, ensure prompt notification to all addressees to whom the information or material was originally transmitted. The notification shall specify the marking action to be taken, the authority therefor, and the effective date. Upon receipt of notification, recipients shall effect the proper changes and shall notify addressees to whom they have transmitted the classified information or material.

(2) *Posted notice.* If prompt remarking of large quantities would be unduly burdensome, the custodian may attach declassification, downgrading, or upgrading notices to the storage unit in lieu of the remarking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, and the storage

units to which it applies. Items withdrawn from such storage units shall be promptly remarked. However, when information subject to a posted downgrading or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

(i) *Foreign Relations Series.* In order to permit the State Department editors of *Foreign Relations of the United States* to meet their mandated goal of publishing 20 years after the event, NASA shall assist these editors by facilitating access to appropriate classified materials in its custody and by expediting declassification review of items from its files selected for publication.

(ii) [Reserved]

[44 FR 34913, June 18, 1979, as amended at 45 FR 3888, Jan. 21, 1980; 48 FR 5892, Feb. 9, 1983; 53 FR 41318, Oct. 21, 1988; 78 FR 5120, Jan. 24, 2013]

EDITORIAL NOTE: At 78 FR 5120, Jan. 24, 2013, §1203.604 was amended in part by revising paragraphs (d)(3) and (4); however, the amendatory instruction could not be incorporated completely because (d)(3) and (4) did not exist.

Subpart G [Reserved]

Subpart H—Delegation of Authority To Make Determinations in Original Classification Matters

SOURCE: 62 FR 54380, Oct. 20, 1997, unless otherwise noted.

§ 1203.800 Establishment.

Pursuant to Executive Order 13526, ''Classified National Security Information,'' and The Space Act, in accordance with U.S.C. Title 51, National and Commercial Space Program Sections 20132 and 20133, there is established a NASA Information Security Program Committee (as part of the permanent administrative structure of NASA). The NASA Assistant Administrator for Protective Services, or designee, shall be the Chairperson of the Committee. The Information Security Program Manager, NASA Office of Protective Services, is designated to act as the Committee Executive Secretary.

[78 FR 5121, Jan. 24, 2013]

§ 1203.801 Responsibilities.

(a) The Chairperson reports to the Administrator concerning the management and direction of the NASA Information Security Program as provided for in subpart B of this part. In this connection, the Chairperson is supported and advised by the Committee.

(b) The Committee shall act on all appeals from denials of declassification requests and on all suggestions and complaints with respect to administration of the NASA Information Security Program as provided for in subpart B of this part.

(c) The Executive Secretary of the Committee shall maintain all records produced by the Committee, its subcommittees, and its ad hoc panels.

(d) The Office of Protective Services will provide staff assistance and investigative and support services for the Committee.

[78 FR 5121, Jan. 24, 2013]

§ 1203.802 Membership.

The Committee membership will consist of the Chairperson, the Executive Secretary, and one person nominated by each of the following NASA officials:

(a) The Associate Administrators for:

(1) Aeronautics.

(2) Science Missions Directorate.

(3) Human Explorations and Operations.

(4) International and Interagency Relations.

(b) The Associate Administrator.

(c) The General Counsel.

(d) The Chief Information Officer.

(e) Other members may be designated upon specific request of the Chairperson.

[78 FR 5121, Jan. 24, 2013]

§ 1203.803 Ad hoc committees.

The Chairperson is authorized to establish such ad hoc panels or subcommittees as may be necessary in the conduct of the Committee's work.

[78 FR 5121, Jan. 24, 2013]

§ 1203.804 Meetings.

(a) Meetings will be held at the call of the Chairperson.

(b) Records produced by the Committee and the minutes of each meeting will be maintained by the Executive Secretary.

[78 FR 5121, Jan. 24, 2013]

Subpart I—NASA Information Security Program Committee

SOURCE: 54 FR 6881, Feb. 15, 1989, unless otherwise noted.

§ 1203.900 Establishment.

Pursuant to Executive Order 13526, ''Classified National Security Information,'' and The Space Act, in accordance with U.S.C. Title 51, National and Commercial Space Program Sections 20132 and 20133, there is established a NASA Information Security Program Committee (as part of the permanent administrative structure of NASA. The NASA Assistant Administrator for Protective Services, or designee, shall be the Chairperson of the Committee. The Information Security Program Manager, NASA Office of Protective Services, is designated to act as the Committee Executive Secretary.

[78 FR 5122, Jan. 24, 2013]

§ 1203.901 Responsibilities.

(a) The Chairperson reports to the Administrator concerning the management and direction of the NASA Information Security Program as provided for in subpart B of this part. In this connection, the Chairperson is supported and advised by the Committee.

(b) The Committee shall act on all appeals from denials of declassification requests and on all suggestions and complaints with respect to administration of the NASA Information Security Program as provided for in subpart B of this part.

(c) The Executive Secretary of the Committee shall maintain all records produced by the Committee, its subcommittees, and its ad hoc panels.

(d) The Office of Protective Services, will provide staff assistance, and investigative and support services for the Committee.

[54 FR 6881, Feb. 15, 1989, as amended at 78 FR 5122, Jan. 24, 2013]

§ 1203.902 Membership.

The Committee will consist of the Chairperson and Executive Secretary. In addition, each of the following NASA officials will nominate one person to Committee membership:

(a) Associate Administrator for:

(1) Aero-Space Technology.

(2) Space Science.

(3) Space Flight.

(4) External Relations.

(5) Life and Microgravity Sciences and Applications.

(b) Associate Deputy Administrator.

(c) General Counsel.

Other members may be designated upon specific request of the Chairperson.

[54 FR 6881, Feb. 15, 1989, as amended at 64 FR 72535, Dec. 28, 1999]

§ 1203.903 Ad hoc committees.

The Chairperson is authorized to establish such ad hoc panels or subcommittees as may be necessary in the conduct of the Committee's work.

§ 1203.904 Meetings.

(a) Meetings will be held at the call of the Chairperson.

(b) Records produced by the Committee and the minutes of each meeting will be maintained by the Executive Secretary.

Subpart J—Special Access Programs (SAP) and Sensitive Compartmented Information (SCI) Programs

SOURCE: 78 FR 5122, Jan. 24, 2013, unless otherwise noted.

§ 1203.1000 General.

A SAP or SCI program shall be created within NASA only upon specific written approval of the Administrator and must be coordinated with the Assistant Administrator for Protective Services, or designee, to ensure required security protocols are implemented and maintained.

§ 1203.1001 Membership.

The Committee membership will consist of the Chairperson, the Executive Secretary, and one person nominated by each of the following NASA officials:

(a) The Associate Administrators for:

(1) Aeronautics.

(2) Science Missions Directorate.

(3) Human Explorations and Operations.

(4) International and Interagency Relations.

(b) The Associate Administrator.

(c) The General Counsel.

(d) The Chief Information Officer.

(e) Other members may be designated upon specific request of the Chairperson.

§ 1203.1002 Ad hoc committees.

The Chairperson is authorized to establish such ad hoc panels or subcommittees as may be necessary in the conduct of the Committee's work.

§ 1203.1003 Meetings.

(a) Meetings will be held at the call of the Chairperson.

(b) Records produced by the Committee and the minutes of each meeting will be maintained by the Executive Secretary.

PART 1203a—NASA SECURITY AREAS

Sec.

AUTHORITY: The National Aeronautics and Space Act of 1958, as amended, 51 U.S.C. 20101 *et seq*.

SOURCE: 38 FR 8056, Mar. 28, 1973, unless otherwise noted.

§ 1203a.100 Purpose and scope.

(a) To insure the uninterrupted and successful accomplishment of the NASA mission, certain designated security areas may be established and maintained by NASA Centers and Component Facilities in order to provide appropriate and adequate protection for facilities, property, or classified/proprietary information and material in the possession of NASA or NASA contractors located at NASA Centers and Component Facilities.

(b) This part sets forth:

(1) The designation and maintenance of security areas,

(2) The responsibilities and procedures in connection therewith, and

(3) The penalties that may be enforced through court actions against unauthorized persons entering security areas.

[38 FR 8056, Mar. 28, 1973, as amended at 78 FR 5123, Jan. 24, 2013]

§ 1203a.101 Definitions.

For the purpose of this part, the following definitions apply:

(a) *Security area.* A physically defined area, established for the protection or security of facilities, property, or classfied/proprietary information and material in the possession of NASA or a NASA contractor located at a NASA Center or Component Facility, entry to which is subject to security measures, procedures, or controls. Security areas which may be established are:

(1) *Controlled area.* An area in which security measures are taken to safeguard and control access to property and hazardous materials or other sensitive material or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. The controlled area shall have a clearly defined perimeter, but permanent physical barriers are not required.

(2) *Limited area.* An area in which security measures are taken to safeguard or control access to classified material or unclassified property warranting special protection or property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. A Limited Area shall also have a clearly defined perimeter, but differs from a Controlled Area in that permanent physical barriers and access control devices, including walls and doors with locks or access devices, are emplaced to assist the occupants in keeping out unauthorized personnel. All facilities